PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-141953
(43)Date of publication of application : 17.05.2002

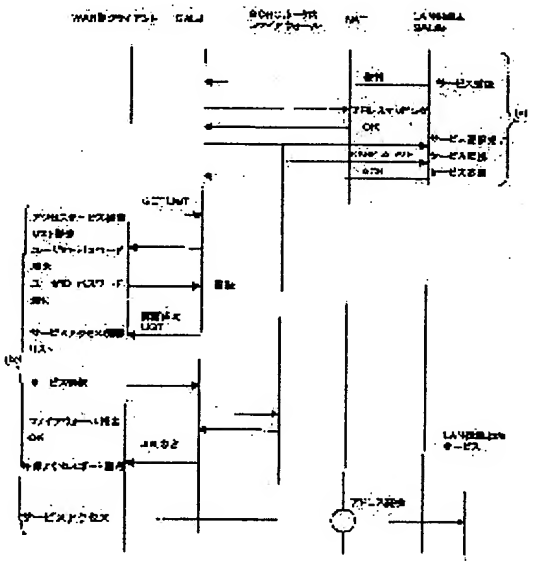
(51)Int.CI. H04L 12/66
G06F 13/00
H04L 12/56
H04L 29/08

(21)Application number : 2000-337392
(22)Date of filing : 06.11.2000

(71)Applicant : SONY CORP
(72)Inventor : ASAI NOBUMASA

(54) COMMUNICATION RELAY DEVICE, COMMUNICATION RELAY METHOD, AND COMMUNICATION TERMINAL, AND PROGRAM STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication network system by which a WAN side terminal can acquire service information of a LAN side terminal and access the LAN side terminal.
SOLUTION: A communication relay device periodically monitors a state of service of terminals under the management of a network connection device acting like a communication relay device such as a router and a gateway to manage the serviceable services by each terminal and provides a serviceable service list to a client requesting an access from an external network such as the Internet in a form of a service access device list, and the network connection device connects the service selected from the list by the client through address conversion. Through the configuration above, the WAN side terminal can access the LAN side terminal by designating a specific service.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－141953
（P2002－141953A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ	12/66		Ｇ０６Ｆ	13/00	３５１Ｚ　５Ｂ０８９
Ｇ０６Ｆ	13/00	３５１			３５３Ｃ　５Ｋ０３０
		３５３	Ｈ０４Ｌ	11/20	Ｂ　５Ｋ０３４
Ｈ０４Ｌ	12/56				１０２Ａ
	29/08			13/00	３０７Ａ

審査請求　未請求　請求項の数18　ＯＬ　（全 16 頁）

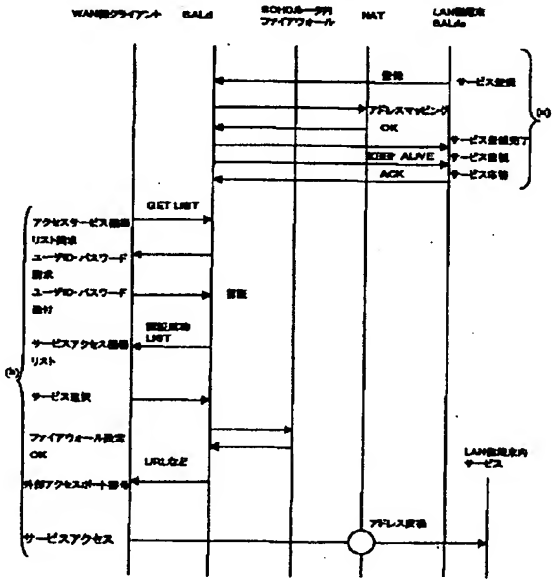
(21)出願番号　特願2000－337392(P2000－337392)
(22)出願日　平成12年11月６日(2000.11.6)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　浅井　伸昌
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　通信中継装置、通信中継方法、および通信端末装置、並びにプログラム配信媒体

(57)【要約】
【課題】　ＷＡＮ側端末からＬＡＮ側端末のサービス情報の取得、およびアクセスを可能とする通信ネットワークシステムを提供する。
【解決手段】　ルータ、ゲートウェイなど、通信中継装置として機能するネットワーク接続機器の管理下の端末のサービスの状態を定期的に監視して、提供可能なサービスを端末毎に管理し、提供可能なサービスリストをインターネット等の外部ネットワークからのアクセスを要求するクライアントに対してサービスアクセス機器リストによって提示し、クライアントがリストから選択したサービスに対して、ネットワーク接続機器がアドレス変換を行なって接続する構成とした。本構成により、ＷＡＮ側からＬＡＮ側へ、特定のサービスを指定したアクセスが可能となる。



【特許請求の範囲】
【請求項１】外部ネットワークとローカルネットワークとの中継手段として機能する通信中継装置であり、
前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を取得し、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示する処理を実行する構成を有することを特徴とする通信中継装置。
【請求項２】前記サービスに対するアクセス情報は、
前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号であることを特徴とする請求項１に記載の通信中継装置。
【請求項３】前記通信中継装置は、
前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を定期的に前記内部端末から受信し、サービス提供可否の状態情報に基づいて端末管理データを更新し、更新した端末管理データに基づいて、外部ネットワークに対して提示するサービス情報とアクセス情報の更新を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項４】前記通信中継装置は、
外部ネットワークを介したクライアントからの前記内部端末に対するアクセス要求に応答して、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号を前記クライアントに提供するとともに、前記クライアントからの外部ポート番号を用いたアクセス要求に応じて、外部ポート番号から内部ポート番号への変換処理を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項５】前記通信中継装置は、
ａ．該中継装置のグローバルＩＰアドレス、
ｂ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号、
ｃ．前記内部端末の個々に設定されたプライベートＩＰアドレス、
ｄ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号、
とを対応付けたネットワークアドレス変換テーブルを有し、
前記通信中継装置は、
前記ネットワークアドレス変換テーブルに基づいて、外部ネットワークを介した内部端末へのアクセス要求中に含まれる中継装置のグローバルＩＰアドレスと外部ポート番号から、プライベートＩＰアドレスと内部ポート番号への変換を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項６】前記通信中継装置は、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントの認証を実行し、認証成立を条件として、前記サービス情報と、該サービスに対するアクセス情報を提示する処理を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項７】前記通信中継装置は、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントのアドレスを設定したファイアウォールを構築して、ファイアウォールに基づくアクセス制限処理を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項８】外部ネットワークとローカルネットワークとの中継手段として機能する通信中継方法であり、
前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を取得するステップと、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示するステップと、
を有することを特徴とする通信中継方法。
【請求項９】前記サービスに対するアクセス情報は、
前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号であることを特徴とする請求項８に記載の通信中継方法。
【請求項１０】前記通信中継方法は、さらに、
前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を定期的に前記内部端末から受信し、サービス提供可否の状態情報に基づいて端末管理データを更新し、更新した端末管理データに基づいて、外部ネットワークに対して提示するサービス情報とアクセス情報の更新を実行することを特徴とする請求項８に記載の通信中継方法。
【請求項１１】前記通信中継方法は、さらに、
外部ネットワークを介したクライアントからの前記内部端末に対するアクセス要求に応答して、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号を前記クライアントに提供するとともに、前記クライアントからの外部ポート番号を用いたアクセス要求に応じて、外部ポート番号から内部ポート番号への変換処理を実行することを特徴とする請求項８に記載の通信中継方法。
【請求項１２】前記通信中継方法は、さらに、
ａ．中継装置のグローバルＩＰアドレス、
ｂ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート

番号とは異なる値に設定された外部ポート番号、
ｃ．前記内部端末の個々に設定されたプライベートＩＰアドレス、
ｄ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号、
とを対応付けたネットワークアドレス変換テーブルに基づいて、外部ネットワークを介した内部端末へのアクセス要求中に含まれる中継装置のグローバルＩＰアドレスと外部ポート番号から、プライベートＩＰアドレスと内部ポート番号への変換を実行することを特徴とする請求項８に記載の通信中継方法。
【請求項１３】前記通信中継方法は、さらに、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントの認証を実行し、認証成立を条件として、前記サービス情報と、該サービスに対するアクセス情報を提示する処理を実行することを特徴とする請求項８に記載の通信中継方法。
【請求項１４】前記通信中継方法は、さらに、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントのアドレスを設定したファイアウォールを構築して、ファイアウォールに基づくアクセス制限処理を実行することを特徴とする請求項８に記載の通信中継方法。
【請求項１５】外部ネットワークとの中継手段として機能する通信中継装置の管理するローカルネットワークに接続された通信端末装置において、
該通信端末装置において提供可能なサービス情報を前記通信中継装置に出力する構成を有することを特徴とする通信端末装置。
【請求項１６】前記サービス情報は、
サービス識別データとサービスに対応する内部ポート番号を含む構成であることを特徴とする請求項１５に記載の通信端末装置。
【請求項１７】前記通信端末装置は、
前記通信中継装置からの要求に応じて、サービス提供可否の状態情報を出力する構成を有することを特徴とする請求項１５に記載の通信端末装置。
【請求項１８】外部ネットワークとローカルネットワークとの中継手段として機能する通信中継システムにおけるデータ通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム記憶媒体であって、前記コンピュータ・プログラムは、
前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を取得するステップと、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示するステップと、
を実行することを特徴とするプログラム記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信中継装置、通信中継方法、および通信端末装置、並びにプログラム記憶媒体に関する。さらに詳細には、プライベートＩＰアドレスとグローバルＩＰアドレスとを対応付けて、双方からの１対１のアクセスを可能とする通信中継装置、通信中継方法、および通信端末装置、並びにプログラム記憶媒体に関する。
【０００２】
【従来の技術】現在、爆発的に普及しているインターネットではルーティングプロトコルとしてＩＰ(InternetProtocol）が用いられている。現在使用されているＩＰはＩＰｖ４であり、発信元／宛先として３２ビットからなるアドレス（ＩＰアドレス）が用いられている。インターネット通信においては、３２ビットＩＰアドレスを各発信元／宛先にユニークに割り当てるグローバルＩＰアドレスを採用し、ＩＰアドレスに応じて、個々の発信元／宛先を判別している。しかし、インターネットの世界は急速に広がりを見せており、ＩＰｖ４の限られたアドレス空間、すなわちグローバルアドレスの枯渇が問題となってきている。これを解決するためにＩＥＴＦ（Internet Engineering Task Force）では、次世代ＩＰアドレスとしてＩＰアドレス空間を３２ビットから１２８ビットに拡張する新しいＩＰｖ６を提案している。しかし、ＩＰｖ６への移行には時間を要し、即効性のある対応にはなり難い。
【０００３】現在のＩＰｖ４を用いながらアドレス空間を広げる手法として、プライベートアドレスを用いる方法が提案されている。プライベートアドレスはグローバルアドレスと異なり、一定の組織内で使用されるアドレスである。例えば、ある企業組織内で任意の数のプライベートアドレスを設定して、個々の社員端末にプライベートアドレスを割り当てることができる。このプライベートアドレスを用いた場合は、外部との接続の際にグローバルＩＰアドレスに変換することが必要となる。それを実現する装置としてＮＡＴ(Network Address Translator）がある。
【０００４】例えば、１つのグローバルＩＰアドレスをＩＳＰ（Internet Service Provider）からもらい、ＬＡＮ内部をＤＨＣＰ（Dynamic Host Configuration Protocol）サーバによってプライベートＩＰアドレスで管理する方法がある。この方式はＬＡＮ(Local Area Network)内部からＷＡＮ（Wide Area Network）へパケットを送出する際、ＳＯＨＯルータでＩＰヘッダのソース（ｓｒｃ）アドレスをＳＯＨＯルータの持つグローバルＩＰアドレスに変換する方法であり、ベーシックＮＡＴと呼ばれる。図１にベーシックＮＡＴ方式を使用したシステムを説明する図を示す。図１において、例えば企業内のプライベートアドレスの割り当てられた端末、ＴＣＰ／ＩＰ（Transmission Control Protocol／Internet Protocol）接続端末１０１～１０ｎがあり、各端末はＬ

ANI20によってNAT130に接続される。NAT130は、インターネット140に接続され、各端末101～10nのIPアドレスはNAT130によってグローバルアドレスに変換される。

【0005】IPアドレスの表記は32ビットのアドレスを8ビットを単位として10進数で表して表記する。NAT130は接続端末101～10nからのパケットに対し、予め設定されている数のグローバルアドレスを先着順に割り当てる。従ってグローバルアドレス設定数以上の通信は並列に実行できないことになる。従って、あくまで並列に実行可能な通信数はグローバルアドレスの数によって制限されてしまう。このようにNATでは1つのプライベートアドレスに対して1つのグローバルアドレスを対応させる処理をしているので、根本的なアドレス枯渇問題を解決するものとはなっていない。

【0006】グローバルIPアドレスをさらに節約するために1個のグローバルIPアドレスの異なるTCPポートを用いて複数のプライベートIPアドレスに対応させる技術も用いられることがある。LAN内部の複数のIP端末からWAN側へパケットを同時に送信出来るように、SOHOルータでsrcアドレスに加えてソース（src）ポートの変換も行い、WAN側からの戻りのパケットをそのsrcポートを見てプライベートIPアドレスに変換する拡張NAT、通称、IPマスカレードという方法である。

【0007】IPマスカレードを用いた通信システム構成を図2に示す。図2においては、インターネット201側にグローバルアドレスが1つあり、例えば企業内のプライベートアドレスの割り当てられた端末であるTCP／IP接続端末が、UDP（User Datagram Protocol）で規定されているポート番号によって識別可能であるとき、TCPやUDPのポート番号を利用することによってそれぞれの端末個々が、1つの共通のグローバルアドレスを利用して通信を実行する構成としたものである。

【0008】IPマスカレードにより、複数の端末からWAN側の同一端末に同時アクセスすることが可能になるが、この方法では最初にLAN側の端末からWAN側の端末へセッションを張らないと、WAN側からLAN内部へのデータ通信が出来ない。NATを使用して、WAN側から最初にLAN側に対してデータ通信を行う方法は、現在提案されていない。さらにいえば、LAN側からWAN側へどのようなサービスが可能であるかについての情報を提供する手段がない。アノニマス（Anonymous）FTPサーバなどをLAN内に立ち上げる例もあるが、このためにはNATにおけるマッピング処理構成を手動で事前に設定しておかなければならない。また、WAN側からアクセスを行なうクライアントもそのサーバの存在を事前に知っておく必要がある。

【0009】

【発明が解決しようとする課題】本発明は、上述のような従来技術の欠点に鑑みてなされたものであり、グローバルアドレスで管理されているWAN側から、プライベートアドレス管理下の登録サービスを利用可能にする通信中継装置、通信中継方法、および通信端末装置、並びにプログラム記憶媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明の第1の側面は外部ネットワークとローカルネットワークとの中継手段として機能する通信中継装置であり、前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を取得し、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示する処理を実行する構成を有することを特徴とする通信中継装置にある。

【0011】さらに、本発明の通信中継装置の一実施態様において、前記サービスに対するアクセス情報は、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号であることを特徴とする。

【0012】さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を定期的に前記内部端末から受信し、サービス提供可否の状態情報に基づいて端末管理データを更新し、更新した端末管理データに基づいて、外部ネットワークに対して提示するサービス情報とアクセス情報の更新を実行する構成を有することを特徴とする。

【0013】さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、外部ネットワークを介したクライアントからの前記内部端末に対するアクセス要求に応答して、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号を前記クライアントに提供するとともに、前記クライアントからの外部ポート番号を用いたアクセス要求に応じて、外部ポート番号から内部ポート番号への変換処理を実行する構成を有することを特徴とする。

【0014】さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、

a．該中継装置のグローバルIPアドレス、b：前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号、c．前記内部端末の個々に設定されたプライベートIPアドレス、d．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号、とを対応付けたネットワークアドレス変換テーブルを有し、前記通信中継装置は、前記ネットワークアドレス変換テーブルに基づいて、外部ネ

ットワークを介した内部端末へのアクセス要求中に含まれる中継装置のグローバルＩＰアドレスと外部ポート番号から、プライベートＩＰアドレスと内部ポート番号への変換を実行する構成を有することを特徴とする。

【００１５】さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントの認証を実行し、認証成立を条件として、前記サービス情報と、該サービスに対するアクセス情報を提示する処理を実行する構成を有することを特徴とする。

【００１６】さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントのアドレスを設定したファイアウォールを構築して、ファイアウォールに基づくアクセス制限処理を実行する構成を有することを特徴とする。

【００１７】さらに、本発明の第２の側面は、外部ネットワークとローカルネットワークとの中継手段として機能する通信中継方法であり、前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を取得するステップと、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示するステップと、を有することを特徴とする通信中継方法にある。

【００１８】さらに、本発明の通信中継方法の一実施態様において、前記サービスに対するアクセス情報は、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号であることを特徴とする。

【００１９】さらに、本発明の通信中継方法の一実施態様において、前記通信中継方法は、さらに、前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を定期的に前記内部端末から受信し、サービス提供可否の状態情報に基づいて端末管理データを更新し、更新した端末管理データに基づいて、外部ネットワークに対して提示するサービス情報とアクセス情報の更新を実行することを特徴とする。

【００２０】さらに、本発明の通信中継方法の一実施態様において、前記通信中継方法は、さらに、外部ネットワークを介したクライアントからの前記内部端末に対するアクセス要求に応答して、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号を前記クライアントに提供するとともに、前記クライアントからの外部ポート番号を用いたアクセス要求に応じて、外部ポート番号から内部ポート番号への変換処理を実行することを特徴とする。

【００２１】さらに、本発明の通信中継方法の一実施態様において、前記通信中継方法は、さらに、ａ．中継装置のグローバルＩＰアドレス、ｂ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号、ｃ．前記内部端末の個々に設定されたプライベートＩＰアドレス、ｄ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号、とを対応付けたネットワークアドレス変換テーブルに基づいて、外部ネットワークを介した内部端末へのアクセス要求中に含まれる中継装置のグローバルＩＰアドレスと外部ポート番号から、プライベートＩＰアドレスと内部ポート番号への変換を実行することを特徴とする。

【００２２】さらに、本発明の通信中継方法の一実施態様において、前記通信中継方法は、さらに、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントの認証を実行し、認証成立を条件として、前記サービス情報と、該サービスに対するアクセス情報を提示する処理を実行することを特徴とする。

【００２３】さらに、本発明の通信中継方法の一実施態様において、前記通信中継方法は、さらに、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントのアドレスを設定したファイアウォールを構築して、ファイアウォールに基づくアクセス制限処理を実行することを特徴とする。

【００２４】さらに、本発明の第３の側面は、外部ネットワークとの中継手段として機能する通信中継装置の管理するローカルネットワークに接続された通信端末装置において、該通信端末装置において提供可能なサービス情報を前記通信中継装置に出力する構成を有することを特徴とする通信端末装置にある。

【００２５】さらに、本発明の通信端末装置の一実施態様において、前記サービス情報は、サービス識別データとサービスに対応する内部ポート番号を含む構成であることを特徴とする。

【００２６】さらに、本発明の通信端末装置の一実施態様において、前記通信端末装置は、前記通信中継装置からの要求に応じて、サービス提供可否の状態情報を出力する構成を有することを特徴とする。

【００２７】さらに、本発明の第４の側面は、外部ネットワークとローカルネットワークとの中継手段として機能する通信中継システムにおけるデータ通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム記憶媒体であって、前記コンピュータ・プログラムは、前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を取得するステップと、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報

と、該サービスに対するアクセス情報とを提示するステップと、を実行することを特徴とするプログラム記憶媒体にある。

【００２８】なお、本発明の第４の側面に係るプログラム記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。

【００２９】このようなプログラム記憶媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該記憶媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３０】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３１】

【発明の実施の形態】［１．システム概要］図３に本発明の通信中継装置および通信端末装置によって構成されるシステムの概要を説明する図を示す。図３は、ＷＡＮ環境としてのインターネットとＬＡＮ環境下の例えばＳＯＨＯ（Small Office/Home Office）とを、通信中継装置であるネットワーク接続機器としてのルータ（ＳＯＨＯルータ）により相互接続した環境、すなわち、インターネットにＩＰ接続されたＳＯＨＯ環境の例である。なお、ここでは、ルータをネットワーク相互間の接続機器の例として説明するが、ゲートウェイその他のネットワーク接続機器も以下の説明と同様の構成を持つ機器として利用可能である。

【００３２】図３に示すように各家庭、Ａさん宅、Ｂさん宅、あるいはその他、各事業所にはインターネット接続された、通信中継装置としてのＳＯＨＯルータ３１０，３２０が各々１台設置されている。そのＳＯＨＯルータはＩＳＰ（Internet Service Provider）などからグローバルＩＰアドレス（ＩＰｖ４）を１つ、もしくは複数個、付与され、その管理下に通信端末装置として複数のＩＰ端末（ＰＣ，モバイル端末など）を管理する。図３では、Ａさん宅のＳＯＨＯルータ３１０に、ＩＰ端末１，３１１とＩＰ端末２，３１２が接続され、Ｂさん宅のＳＯＨＯルータにＩＰ端末としてＨＴＴＰサーバ３２１、ＦＴＰサーバ３２２、ＲＴＳＰサーバ３２３が接続された例を示している。

【００３３】図３の例では、Ａさん宅のＳＯＨＯルータ３１０にはグローバルＩＰアドレス［４３．１１．ＸＸ．ＸＸ］が設定され、Ｂさん宅のＳＯＨＯルータ３２０にはグローバルＩＰアドレス［４３．１０．ＸＸ．ＸＸ］が設定されている。ここで、ＳＯＨＯルータは、アクセス要求の各ホストに動的にＩＰアドレスを割り当てるＤＨＣＰ（Dynamic Host Configuration Protocol）サーバの機能と、ドメイン名とＩＰアドレスとの対応付け処理を実行するＤＮＳ（Domain NameSystem）サーバとしての機能を兼務する。各ＳＯＨＯルータ３１０，３２０の管理下のＩＰ端末は、ＳＯＨＯルータにより割り当てられるＩＰアドレスによってルーター、インターネットを介した外部端末との接続が可能となり、様々な処理、例えばメール転送、画像転送などが可能となる。

【００３４】ＳＯＨＯルータ３１０，３２０は、ＩＰ端末接続時にそのプライベートＩＰアドレスを管理下の各端末３１１，３１２，３２１，３２２，３２３に割り振り、その名前を登録する。各ＳＯＨＯルータ管理下のＩＰ端末では、ＦＴＰ(File Transfer Protocol)、ＨＴＴＰ（Hyper Text Transfer Protocol）、ＲＴＳＰ(Real-time Streaming Protocol)などのサービスを提供することができる。

【００３５】図３の例では、Ａさん宅のＳＯＨＯルータ３１０は、管理下のＩＰ端末にプライベートＩＰアドレスとして、ＩＰ端末１，３１１に［１９２．１６８．０．２］、ＩＰ端末２，３１２に［１９２．１６８．０．３］を設定し、Ｂさん宅のＳＯＨＯルータ３２０は、管理下のＩＰ端末にプライベートＩＰアドレスとして、ＨＴＴＰサーバ３２１に［１９２．１６８．０．２］、ＦＴＰサーバ３２２に［１９２．１６８．０．３］、ＲＴＳＰサーバ３２３に［１９２．１６８．０．４］を設定している。

【００３６】［２．サービス登録］本発明の通信中継装置であるネットワーク接続機器としての図３の構成におけるＳＯＨＯルータ３１０，３２０は、各ＳＯＨＯルータ管理下のＩＰ端末３１１，３１２、３２１，３２２，３２３のＳＯＨＯルータ接続時に、その端末で現在提供可能なサービスをＳＯＨＯルータ上のサービスアクセス機器リスト管理デーモン（以下、省略してＳＡＬｄ（Service Access Device List Demon）と呼ぶ）に登録する。なお、デーモンとは、システム常駐プログラムであり、アプリケーション・プログラム、またはシステムの状態に応じて自動的に特定の処理を実行するプログラムである。

【００３７】本発明の通信中継装置であるネットワーク接続機器（ｅｘ．ルータ、ゲートウェイなど）に設定されるＳＡＬｄは、ＳＯＨＯ環境において各ＩＰ端末の提供できるサービスを階層的に管理したり、そのサービス内容を動的に更新したり、それをＷＡＮ側に提示する処理を実行するプログラムである。

【００３８】一方、ＳＡＬｄのを有するネットワーク接続機器の管理下のＩＰ端末には、サービス監視デーモン（ＳＡＬｄクライアント、略してＳＡＬｄｃと呼ぶ）が設定されている。ＳＯＨＯルータ等のネットワーク接続

機器のSALdは各IP端末上のサービス監視デーモン（SALdc）からサービス登録メッセージ（REGISTER）をネットワーク接続、あるいはIP端末の電源投入時に受け取る。SALdは内部管理下のすべてのSALdcからのサービス登録メッセージ（REGISTER）を受け取り、それを端末別に階層的に管理する。

【0039】SOHO環境のLAN側のプライベートIPアドレスを使用した端末のサービスの階層的管理の例としては、例えば、LAN内にアプリケーションゲートウェイなどの機能を持つPCがいて、そのPCの管理下に非IP機器（例えば1394、USBなどの独自データリンクをもつ）が接続された環境における機器の管理の場合などがある。図4に階層構成を持つ機器接続システム例を示す。

【0040】図4のシステムは、インターネットにネットワーク接続機器としてのSOHOルータ401が接続され、その下位にIP端末としてのPC1，402，アプリケーションゲートウェイ機能を持つPC2，403が接続され、PC2，403の下位に非IP端末として、1394パスに接続されたカメラ404，デッキ405、さらにUSB接続機器406が接続された構成である。

【0041】非IP機器が行うサービスは、IP端末のPC2，403の下の階層の機器のサービスであり、例えば1394のDVカメラなどの映像サービス、デッキの映像サービス等である。ネットワーク接続機器としてのSOHOルータ401は、IP端末、非IP端末の提供サービスを登録して階層的管理を行なうことができる。

【0042】図5に1つのIP端末上に複数のサービスが存在する場合の、サービス登録の方法を示す。図5は、図3におけるAさん宅のシステム構成を示している。IP端末1，311ではFTP(File Transfer Protocol)、HTTP（Hyper Text Transfer Protocol）、何かしらのその端末独自なサービスが起動されており、端末2，312ではHTTP、RTSP(Real-time Streaming Protocol)のサービスが起動されているとする。

【0043】IP端末1，311は、サービス監視デーモン（SALdc）の監視により、起動中のサービス（アプリケーション）情報を取得して、<サービス名、内部ポート番号>として、{<FTP，20>、<HTTP，80>、<独自サービス、6001>を得ており、また、IP端末2，312では{<HTTP，80>、<RTSP，554>}を取得している。各IP端末は、これらの起動サービス（アプリケーション）情報をそれぞれ、ネットワーク接続機器（SOHOルータ）のSALdにREGISTER（登録）する。

【0044】IP端末1，311の、サービス監視デーモン（SALdc1）からSOHOルータ310に送信される登録メッセージ（REGISTER）例を図6に示す。

【0045】図6に示すように、登録メッセージは、端末に割り当てられたプライベートIPアドレス、端末名、端末属性、サービス名、サービス属性、内部ポート番号によって構成される。プライベートIPアドレスは、SOHOルータ310によって付与されたIPアドレスである。端末名は、SOHOルータ310管理下の各端末を識別する識別名であり、端末属性は、PC（Personal Computer）などの機器の種別を示す。インターネット接続可能な例えばテレビ、ビデオ、サーバ、その他家電製品などIPアドレスの設定により通信可能な機器の種類を示すデータである。サービス名は、IP端末において提供するサービス（アプリケーション）を示している。図6の例では、IP端末1，311は、FTP(File Transfer Protocol)、HTTP（Hyper Text Transfer Protocol）、その他の独自サービスを提供可能なPCである。サービス属性は、FTP，HTTP，独自サービスのサービスの態様を示している。内部ポート番号は、各サービスを識別するための番号として、各サービスに対して設定された番号である。

【0046】ネットワーク接続機器（ex．ルータ、ゲートウェイなど）のSALdは、図6に示すような登録メッセージを受領して、管理データ（図8参照）として登録する。

【0047】［3．サービスの更新］ネットワーク接続機器（ex．ルータ，ゲートウェイ）のSALdは、管理下IP端末の各SALdcとの間で、定期的なサービスの情報交換を行い、IP端末の提供サービスの内容を更新する。ネットワーク接続機器（ex．ルータ，ゲートウェイ）のSALdは管理下IP端末のSALdcに対して、管理下IP端末の管理データに登録済みのサービスが有効に利用可能であるかのチェックを定期的、例えば30秒単位で行なう。

【0048】ネットワーク接続機器（ex．ルータ，ゲートウェイ）のSALdは、管理下IP端末のサービスアクセス機器リストに登録済みのサービス内容を示すメッセージ（KEEP ALIVE）を送信し、管理下IP端末のSALdcはメッセージ（KEEP ALIVE）を受信し、そのサービスが端末側で提供可能であればACKを返す。SALdは所定時間までこのACKを待って、受信できない場合はその内容をサービスアクセス機器リストから削除する。また、SALdcはIP端末で新たに起動されたサービスを監視し、SALdにREGISTERメッセージを送信する。

【0049】［4．NATへのサービスマッピング］ネットワーク接続機器（ex．ルータ，ゲートウェイ）のSALdは管理下のIP端末の提供可能な各種サービス内容をWAN側のクライアントに提示するためのサービスマッピングを行う。LAN側の各IP端末は、プライ

ベートＩＰアドレスで管理されているため、WAN側から各ＩＰ端末を直接アクセスすることができない。従って、ＬＡＮ内の接続ＩＰ端末で提供するサービスをWAN側クライアントがＬＡＮ内の接続ＩＰ端末に直接問い合わせを行なうことはできない。

【００５０】WAN側クライアントがＬＡＮ内の接続ＩＰ端末の提供サービスを知り、サービスを実行させるためには、ＩＰ端末を管理するネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）に割り当てられたグローバルＩＰアドレスから、対応するＩＰ端末のプライベートアドレスに変換させる必要がある。各ＩＰ端末では、図６の登録メッセージの例で示したように、ＦＴＰ，ＨＴＴＰ…など、複数のサービスを提供する可能性があるので、ＩＰアドレスだけではなく、各サービスのポート番号情報も必要である。

【００５１】ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄでは管理下ＩＰ端末の提供するサービスに対応するWAN側に見せる外部ポートを決定し、ＳＯＨＯルータのグローバルＩＰアドレス、外部ポート宛てに到達したパケットのＩＰヘッダの宛先アドレス／ポート番号（ｄｅｓｔｉｎａｔｉｏｎ ａｄｄｒｅｓｓ／ｐｏｒｔ）を、各ＩＰ端末のプライベートＩＰアドレス、サービスの内部ポート番号に書き換える様、ＮＡＴ(Network Address Translator)に設定する。ＮＡＴに設定する変換テーブルの例を図７に示す。

【００５２】図７の例は、図５のシステムにおけるＳＯＨＯルータ３１０に設定される変換テーブルの例である。図７に示すように、ＮＡＴ変換テーブルには、変換前宛先ＩＰアドレス、変換前宛先ポート番号、変換後宛先ＩＰアドレス、変換後宛先ポート番号が設定される。

【００５３】変換後宛先ＩＰアドレスは、ネットワーク接続機器（ＳＯＨＯルータ）３１０がＩＰ端末１，３１１、およびＩＰ端末２，３１２に割り当てているプライベートＩＰアドレスであり、また、変換後ポート番号は、各ＩＰ端末の提供サービスに対応付けられた内部ポート番号である。これらは、先に説明した図６の登録メッセージに基づくリストから取得できる。

【００５４】変換前宛先ＩＰアドレスは、ＳＯＨＯルータ３１０のグローバルＩＰアドレスである。変換前宛先ポート番号は、ＳＯＨＯルータ３１０の管理ＩＰ端末の提供するサービス毎にＳＯＨＯルータが設定する外部ポート番号である。

【００５５】ネットワーク接続機器としてのＳＯＨＯルータのＮＡＴ、ＳＡＬｄとの処理について具体的に説明する。ＳＯＨＯルータのＳＡＬｄは、内部データとして、図８に示す端末管理データを持つ。

【００５６】図８の例は、図５のシステムにおけるＳＯＨＯルータ３１０に設定される端末管理データの例である。図８の端末管理データには、端末に割り当てられたプライベートＩＰアドレス、端末名、端末属性、サービス名、サービス属性、外部ポート番号、内部ポート番号によって構成される。これらのデータは、先に図６を用いて説明した各管理ＩＰ端末からの登録メッセージに基づいて生成される。

【００５７】プライベートＩＰアドレスは、ＳＯＨＯルータ３１０によって付与されたＩＰアドレスである。端末名は、ＳＯＨＯルータ３１０管理下の各端末を識別する識別名であり、端末属性は、ＰＣ（Personal Computer）などの機器の種別を示す。サービス名は、ＩＰ端末において提供するサービス（アプリケーション）を示している。サービス属性は、ＦＴＰ，ＨＴＴＰ，独自サービスのサービスの態様を示している。外部ポート番号は、WAN側クライアントに提示スルために、ＳＯＨＯルータで決めたサービスを識別する番号である。内部ポート番号は、各サービスを識別するための番号として、各サービスに対して設定された番号である。

【００５８】この例では、ＩＰ端末１，３１１のＦＴＰ、ＨＴＴＰ、独自サービスに対して、外部ポートアドレスがそれぞれ８０００、８００１、８００２が割り当てられており、同様にＩＰ端末２，３１２のＨＴＴＰ、ＲＴＳＰに対して、外部ポートアドレスがそれぞれ８００３、８００４が割り当てられている。この外部に割り当てるポート番号は、カーネルなどが使用しない領域をＳＡＬｄが自由に設定できるものとし、サービスが終了した場合などはこのポート番号はプール領域に戻される。また、サービスによっては（例えばメッセージペイロード内にサービスの提供ポート番号など埋め込むＲＴＳＰやＦＴＰなど）、外部からの接続先である外部ポートを指定してＲＥＧＩＳＴＥＲすることができる。これにより、ＮＡＴ変換前のポート番号が指定でき、事前にＲＴＳＰなどのメッセージペイロードにその指定したポート番号を埋め込むことが出来る。

【００５９】［５．サービスアクセス機器リスト］ネットワーク接続機器としてのＳＯＨＯルータのＳＡＬｄは図８に示す端末管理データを保持し、WAN側にいるクライアントからそのＳＯＨＯルータの管理ＩＰ端末に対するサービス要求があった場合、図９に示すようなサービスアクセス機器リストを返す。

【００６０】図９に示すように、サービスアクセス機器リストには、ネットワーク接続機器としてのＳＯＨＯルータの管理するＩＰ端末情報として、端末名、端末属性、サービス名、サービス属性が含まれる。

【００６１】サービスアクセス機器リストには、上述のようにそのＳＯＨＯ環境内にある端末の名前、その端末の属性、サービス名、そのサービスの属性などの項目が含まれる。WAN側にいるユーザにどのようなネットワーク機器が存在し、その上でどのようなサービスが稼動しいるかを知らしめるためである。また、サービスアクセス機器リスト作成時に、ＮＡＴによるアドレス変換は設定するが、まだこの時点では、WAN側からの各種サ

ービスに対するファイアウォールの設定を禁止しておく。

【0062】WAN側クライアントは、図9に示すサービスアクセス機器リストから、サービスを選択し、選択サービスをネットワーク接続機器としてのSOHOルータに通知し、SOHOルータは、選択サービスに対応する外部ポート番号を要求クライアントに提供する。SOHOルータ310は、WAN側クライアントのグローバルIPアドレスと外部ポート番号（変換前宛先ポート番号）に基づくアクセス要求を図7のNAT変換テーブルに基づいて、IP端末のプライベートIPアドレスと、変換後ポート番号に変換する。

【0063】なお、サービスアクセス機器リストは、WAN側にいる認証されたユーザに対してのみ提示する構成とするのが望ましい。また、認証されたユーザをユーザ登録データとして保持し、ユーザ毎に全てのサービス情報を表示したり、特定のサービスのみを抜き出して、特定の端末の情報だけを収集して、ユーザ固有のサービスアクセス機器リストを生成して提示する構成としてもよい。

【0064】[6. SALdの処理] ネットワーク接続機器（ex. ルータ, ゲートウェイ）のSALdの実行するサービス登録フローを図10に示す。まず、定期的に発行されるSALdイベントを取得（S101）すると、管理下のIP端末からの新規サービス登録メッセージがあるか否かを検証（S102）し、ある場合は、登録メッセージに対する外部ポートを設定（S103）し、NAT変換テーブルを設定する。これは、図7のテーブルを生成する処理である。

【0065】NAT変換テーブルの設定が成功すると、登録完了通知をIP端末に送信（S105）し、登録IDを決定し、サービスの監視処理イベントをタイマー管理を開始（S106）し、端末管理データ（図8参照）を生成（S107）する。NAT変換テーブルの生成に失敗した場合は、登録失敗を送信し（S108）、フローの先頭に戻る。

【0066】ステップS102において、新規サービス登録処理でないと判定した場合は、サービス登録IP端末に対するサービスの提供可否の問い合わせとして実行される［KEEP ALIVE］に対する応答［ACK］の受信であるかを判定（S109）する。IP端末は、サービス提供可否の状態情報としてサービス提供可である場合はACKを出力する。ネットワーク接続機器のSALdは、IP端末からACK受信をした場合は、登録サービスに対するACKであるか否かを検証（S110）し、登録サービスである場合は、タイマーのリセット（S111）を行なう。登録サービスに対するACKでない場合は、無効（S112）として扱う。

【0067】ステップS109において、［KEEP ALIVE］に対する応答［ACK］の受信でないと判定されると、タイマーイベントであるか否かが判定（S113）され、タイマーイベントである場合は、図11のタイマー処理（S114）が実行される。

【0068】図11のタイマーイベント処理について説明する。まずタイマーが0であるか否かが判定（S202）され、0である場合は、登録IP端末に対するサービスの提供可否の問い合わせとして実行される［KEEP ALIVE］をIP端末に送信（S203）する。次に、タイマーが予め定めたIP端末からのACK応答待機時間を超えたか否かを判定（S204）し、超えた場合には、ネットワーク接続機器（ex. ルータ, ゲートウェイ）のSALdの管理する端末管理データ（図8参照）から、登録サービスを削除（S205）し、タイマーを更新（S206）する。なお、図11でのタイマーイベントは、登録IP端末に対するサービスの提供可否の問い合わせとして実行される［KEEP ALIVE］発行処理で起動する周期割り込みイベントである。

【0069】[7. ユーザ認証] SALdは、ネットワーク接続機器（ex. SOHOルータ）のある予約ポートとしてのウェルノウンポート（Well Known Port）にTCP／UDPコネクトするデーモンである。従って、SOHOルータのアドレス（グローバルIPアドレス）とそのポート番号が知られてしまえば、WAN側のいかなる悪意をもったユーザからもアクセスできてしまう。しかし、図9用いて説明したサービスアクセス機器リストに関しては、SOHO環境内の個人もしくは事業主の秘密情報である。ましては外部からそのネットワーク機器にアクセスでき、コントロールされてしまうのはもっての他である。

【0070】従って、本システムにおいては、WAN側クライアントからネットワーク接続機器（ex. SOHOルータ）のSALdに対するアクセス時に認証を実行する。具体的には、HTTPd（HTTPデーモン）などが実装しているユーザ、パスワードによる認証を使用し、SALdアクセス時にCGI（Common Gateway Interface）などを使用し、HTTPdサーバが認証を行うディレクトリ以下にアクセスするように構成する。このディレクトリでの認証を事前に登録してあるユーザ名、パスワードにて行い、許可されたユーザに対してのみ、サービスアクセス機器リストを提供する構成とする。

【0071】従って、ユーザ認証を行なうネットワーク接続機器としての例えばSOHOルータの管理下のIP端末に接続するためには、SOHOルータに対するユーザ登録を必要とする。なお、フリーなアクセスを許容する環境であれば必ずしもユーザ登録、認証処理を実行する必要はない。

【0072】[8. サービスの選択、ファイアフォールの設定] WAN側にいる認証されたユーザは、HTTPなどを拡張したプロトコルを使用してSALdからサービスアクセス機器リスト（図9参照）を取得することが

できる。このリストはHTMLなどを使用して書かれており、ユーザはその中から指定したサービス項目を選択することができる。SALdがユーザの指定したサービス項目を受け取った時点で、SOHOルータ内のファイアフォールに対して、そのユーザからのセッションの送信元（src）IPアドレス（および送信元（src）ポート番号）と、ネットワーク接続機器（ex.ルータ、ゲートウェイ）の提供するサービスアクセス機器リストにより指定したサービスに対応する宛先ポート番号（外部ポート番号）の組み合わせで、その通信に対してのアクセスを許可する。例えば、WAN側にいるクライアント（IPアドレスが43.10.133.89）が図9に示すサービスアクセス機器リストのうち、IP端末1のFTPサービスを選択したとすると、図12に示すようなファイアウォールの設定が可能となる。なお、43.11.135.87はSOHOルータのグローバルIPアドレスとする。

【0073】図12のファイアウォールは、送信元IPアドレスが[43.10.133.89]のユーザに対して外部ポート番号8000のサービス、すなわち、図8に示す管理データから理解されるように、IP端末1のFTPサービスを許可するファイアウォールである。

【0074】ちなみにファイアフォールの設定は、WAN側からLAN側への通信は、原則として事前に禁止しておく。これにより、認証されたユーザの選択したサービスに対して、そのユーザの属する端末（場合によってはセッション）からのアクセスしか許可しないことになり、SOHO環境内の機器に対する外部からのアクセスに対するセキュリティを強化することができる。

【0075】このように、本発明のシステムではWAN側にいる認証されたユーザがサービスを選択した時点で、SOHOルータ内にあるファイアフォールに対して、選択したユーザの端末IPアドレス、SOHOルータのグローバルIPアドレス、サービスへの外部ポート番号の組を設定してアクセスを許可する構成とした。従って、外部クライアントは、SOHOのLAN内の機器に対するルータの許可のない制御は不可能であり、高度なセキュリティ管理が可能となる。

【0076】[9.WAN側ユーザからのSOHO環境内サービスへのアクセス]ネットワーク接続機器（ex.ルータ、ゲートウェイ）のSALdは、サービスアクセス機器リストに基づくWAN側クライアントからの、提供サービスの選択を受けて、ファイアフォールを設定後、そのサービスに対する外部ポート番号をユーザに伝達する。ユーザはその外部ポート番号で、例えば、http://43.11.135.87:8000などのURLで、その指定したサービスにアクセス可能になる。上記URLの[43.11.135.87]は、SOHOルータのグローバルIPアドレスであり、[8000]は、サービスに対応する外部ポート番号である。

【0077】SOHOルータは、上記URLを前述のNAT変換テーブル（図7）に基づいて、サービスを提供するIP端末のプライベートアドレスと、内部ポート番号に変換して、接続を実行する。

【0078】[10.セッションの開始]WAN側クライアントがネットワーク接続機器（ex.ルータ、ゲートウェイ）のSALdから教えられたURLなどを使用して、SOHO環境内サービスとセッションを確立し、通信を開始する。

【0079】図13に、ネットワーク接続機器（ex.ルータ、ゲートウェイ）のSALdによるLAN側の内部端末のサービス登録処理、WAN側端末からのアクセス要求に対する処理をまとめたシーケンス図を示す。

【0080】図13の上段（a）は、ネットワーク接続機器（ex.ルータ、ゲートウェイ）のSALdの管理IP端末のサービス登録処理である。

【0081】まず、登録要求がIP端末のSALdcからネットワーク接続機器（ex.ルータ、ゲートウェイ）のSALdに送信される登録メッセージは、図6に示す通りである。SALdは、登録メッセージに基づいて、管理データ（図8）を生成し、NAT変換テーブル（図7）を生成し、登録完了メッセージをIP端末のSALdcに送信する。その後は、定期的にサービスの起動状況をKEEP ALIVEの送信、IP端末からのACK受信により監視し、ACKがなかった場合には、管理データから登録サービスを削除する。IP端末のSALdcは、サービス提供可否の状態情報としてサービス提供可である場合にのみACKをSALdに対して出力する。

【0082】図13の（b）は、WAN側クライアントからのサービス・リクエストに対する処理を示している。WAN側クライアントは、ネットワーク接続機器（ex.ルータ、ゲートウェイ）に対してサービスアクセス機器リスト（図9）の提供を要求すると、SALdは、要求クライアントに対してユーザID，パスワードの入力を求め、入力されたユーザID．パスワードによる認証処理を実行する。なお、認証の形態は、セキュリティレベルに応じてその他の認証方法、例えば公開鍵暗号方式、共通鍵暗号方式などを適用してもよい。

【0083】認証が成功すると、SALdは、要求クライアントに対してサービスアクセス機器リスト（図9）を提供する。クライアントは、リストに基づいてサービスを選択し、SALdは、クライアントのIPアドレス（送信元アドレス）と選択サービスに従って、ファイアウォール（図12参照）を設定する。

【0084】その後、SALdは、要求クライアントに対して、要求のあったサービスに対するアクセスに必要な情報としてURL、具体的には、ネットワーク接続機器ex.ルータ、ゲートウェイ）のグローバルアドレ

ス、サービスに対応する外部ポート番号を設定したＵＲＬを提供する。

【００８５】ＷＡＮ側クライアントは、提示されたＵＲＬに基づいて、ＬＡＮ側ＩＰ端末のサービスに対するアクセスを実行する。なお、この際ＮＡＴにおいて、図７に示すＮＡＴ変換テーブルを用いたアドレス変換として、プライベートＩＰアドレスと内部ポート番号へ変換が実行される。

【００８６】このように、本発明のシステムによれば、ルータ、ゲートウェイなど、通信中継装置であるネットワーク接続機器の管理下の端末のサービスの状態を定期的に監視して、サービスが不可能になった場合、あるいは新たなサービスが追加された場合などにその状態を更新し、常に最新の状態に保持したデータを保有する構成とするとともに、インターネット等の外部ネットワークからのアクセスを要求するクライアントに対してアクセス可能なサービスの情報をサービスアクセス機器リストによって提示し、選択したサービスに対して、ネットワーク接続機器がアドレス変換を行なって接続する構成としたので、ＷＡＮ側からＬＡＮ側へ、特定のサービスを指定したアクセスが可能となる。

【００８７】なお、以上の構成は、ＩＰｖ４アドレス環境固有というものではなく、ＩＰｖ６環境に移行することなったとしても、ＳＯＨＯのＬＡＮ内部のネットワーク環境を外部に公開したくないという要求は同じであり、その場合、ＬＡＮ内部をＩＰｖ６リンクローカルアドレスで管理することになり、外部と直接インターネット接続を行わない構成となり、ＬＡＮ内部のサービス情報をＷＡＮ側のアクセス権限のあるユーザに見せる処理構成としては、上述した本発明の構成が適用可能である。

【００８８】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【発明の効果】以上説明してきたように、本発明の通信中継装置、通信中継方法、通信端末装置、並びにプログラム記憶媒体によれば、ルータ、ゲートウェイなど、ネットワーク接続機器の管理下の端末のサービスの状態を定期的に監視して、提供可能なサービスを端末毎に管理し、提供可能なサービスリストをインターネット等の外部ネットワークからのアクセスを要求するクライアントに対してリストによって提示し、クライアントの選択したサービスに対して、ネットワーク接続機器がアドレス変換を行なって接続する構成としたので、ＷＡＮ側からＬＡＮ側へ、特定のサービスを指定したアクセスが可能となる。

【００８９】また、本発明の構成によれば、通信端末装置のサービスが不可能になった場合、あるいは新たなサービスが追加された場合などにその状態を更新し、常に最新の状態に保持したデータを保有する構成としたので、動的なＩＰ端末サービス管理が実行可能となる。

【００９０】また、本発明の構成によれば、ＷＡＮ側からのクライアントに対しては、認証を行なって認証が成立した場合にのみサービスアクセス機器リストを提示する構成としたので、不正なユーザによる内部環境の漏洩が防止される。

【００９１】

【図面の簡単な説明】

【図１】従来のＮＡＴを用いたプライベートアドレスとグローバルアドレス間でのデータ通信態様を説明する図である。

【図２】従来のＩＰマスカレードを用いたプライベートアドレスとグローバルアドレス間でのデータ通信態様を説明する図である。

【図３】本発明のシステム構成の例を示す図である。

【図４】本発明のシステム構成としての階層構成の例を示す図である。

【図５】本発明のサービスアクセス機器リスト管理デーモン（ＳＡＬｄ）とサービス監視デーモン（ＳＡＬｄｃ）の実行するサービス登録処理を説明する図である。

【図６】本発明のサービスアクセス機器リスト管理デーモン（ＳＡＬｄ）とサービス監視デーモン（ＳＡＬｄｃ）の実行するサービス登録処理における登録メッセージ例を示す図である。

【図７】本発明の構成におけるネットワーク接続機器の有するＮＡＴ変換テーブルの例を示す図である。

【図８】本発明の構成におけるネットワーク接続機器の有する端末管理データの例を示す図である。

【図９】本発明の構成におけるネットワーク接続機器が提供するサービスアクセス機器リストの例を示す図である。

【図１０】本発明の構成におけるネットワーク接続機器の実行するサービス登録処理、更新処理を説明するフロー図である。

【図１１】本発明の構成におけるネットワーク接続機器の実行するサービス登録処理、更新処理におけるタイマー処理を説明するフロー図である。

【図１２】本発明の構成におけるネットワーク接続機器の生成するファイアウォールの例を示す図である。

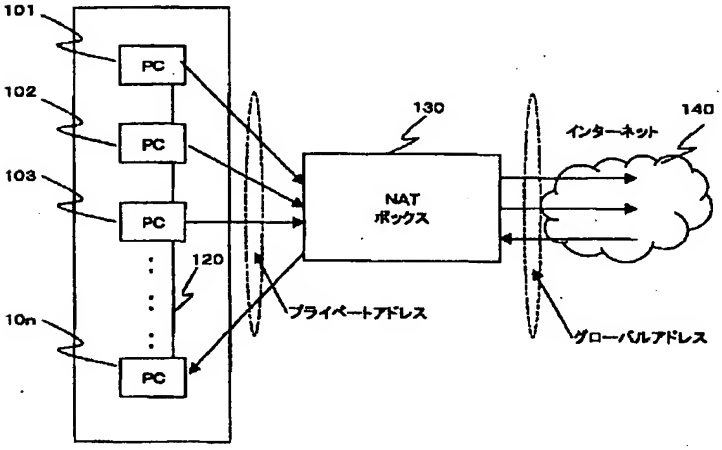
【図１３】本発明の構成におけるネットワーク接続機器の実行する処理シーケンスを示す図である。

【符号の説明】

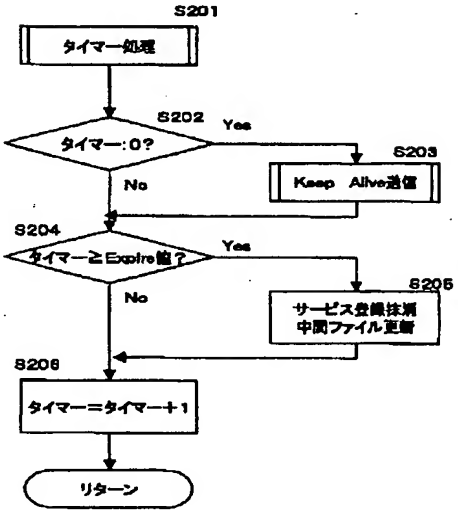
１０１～１０ｎ　通信端末
１２０　ＬＡＮ
１３０　ＮＡＴボックス
１４０　インターネット

201～20n　通信端末
220　LAN
230　IPマスカレードボックス
240　インターネット
310　SOHOルータ
311　IP端末1
312　IP端末2
320　SOHOルータ
321　HTTPサーバ
322　FTPサーバ
323　RTSPサーバ
401　SOHOルータ
402　PC1
403　アプリケーションゲートウェイPC2
404　カメラ
405　デッキ
406　USB機器

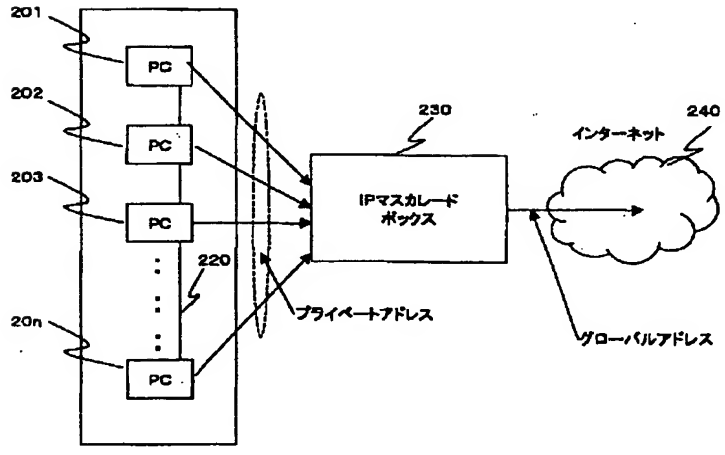
【図1】



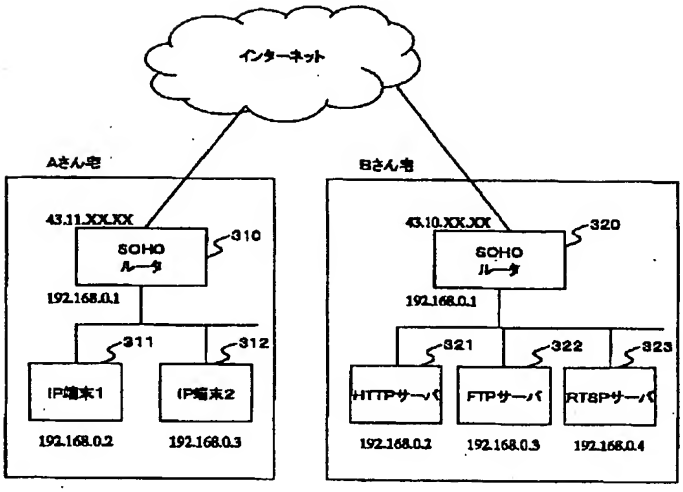
【図11】



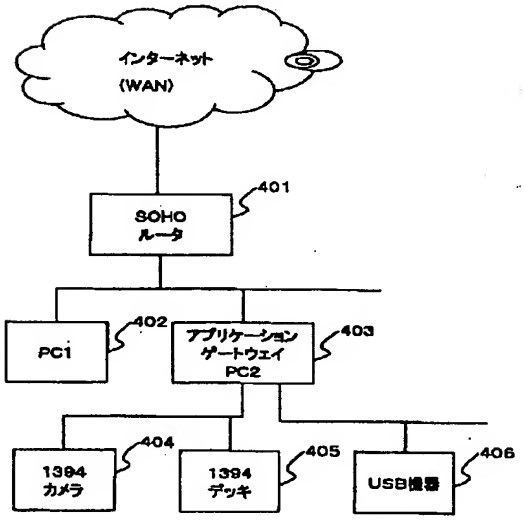
【図2】



【図３】



【図４】



【図７】

NAT変換テーブル

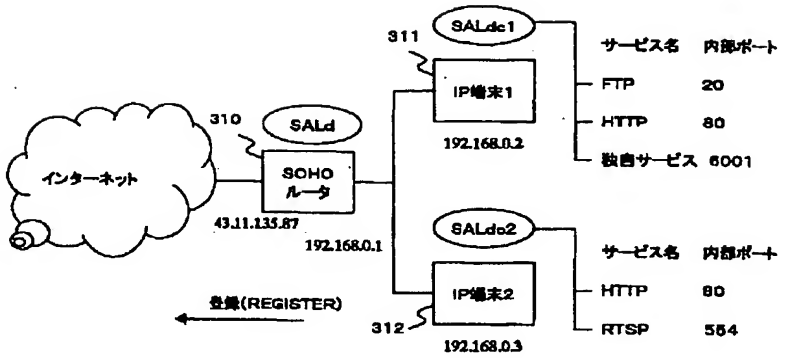
変換前 宛先IPアドレス	変換前 宛先ポート番号 (外部ポート番号)	変換後 宛先IPアドレス	変換後 宛先ポート番号 (内部ポート番号)
43.11.135.87	8000	192.168.0.2	20
43.11.135.87	8001	192.168.0.2	60
43.11.135.87	8002	192.168.0.2	6001
43.11.135.87	8003	192.168.0.3	80
43.11.135.87	8004	192.168.0.3	554

【図１２】

ファイアウォール

送信元IPアドレス	宛先IPアドレス	宛先ポート番号	動作
43.10.133.89	43.11.135.87	8000	通過許可
−	43.11.135.87	−	通過禁止

【図5】



【図6】

登録メッセージ

プライベートIPアドレス	端末名	端末属性	サービス名	サービス属性	内部ポート番号
192.168.0.2	IP端末1	PC	FTP	データ転送	20
192.168.0.2	IP端末1	PC	HTTP	インターネット	80
192.168.0.2	IP端末1	PC	独自サービス	映像、音声	6001

【図8】

端末管理データ

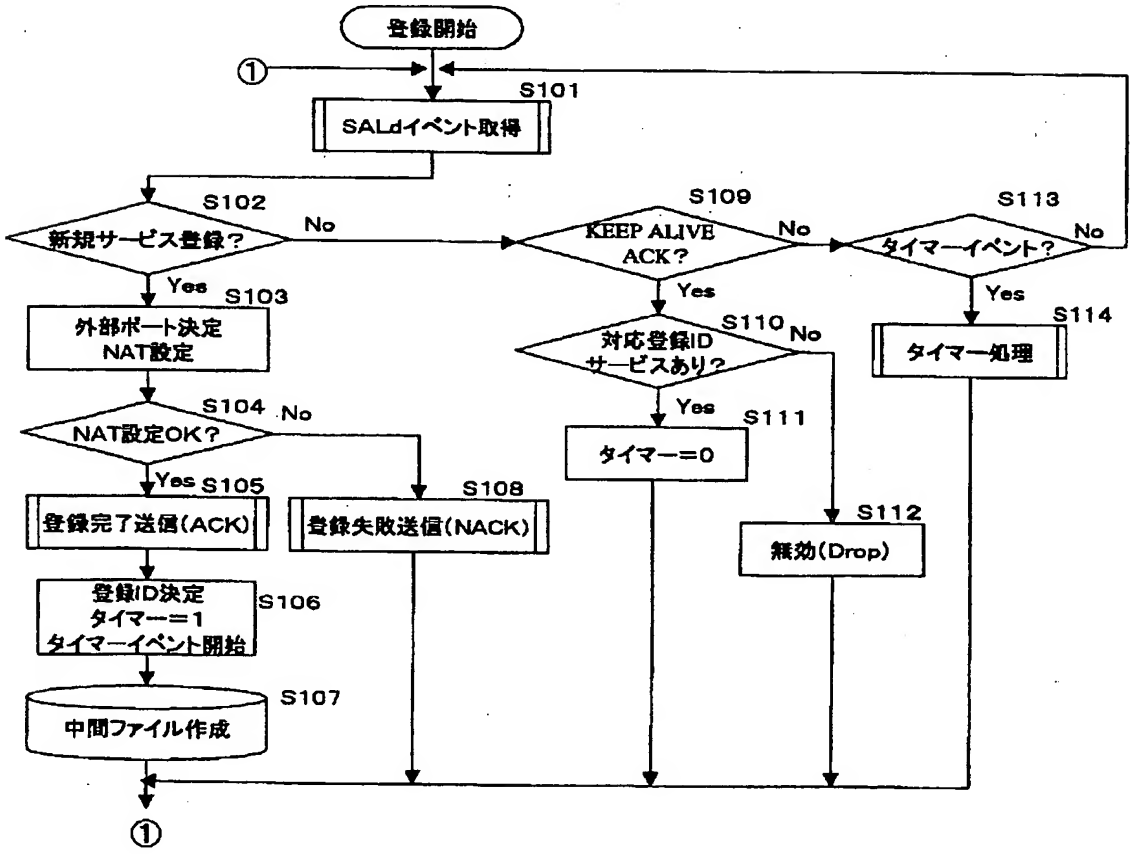
プライベートIPアドレス	端末名	端末属性	サービス名	サービス属性	外部ポート番号	内部ポート番号
192.168.0.2	IP端末1	PC	FTP	データ転送	8000	20
192.168.0.2	IP端末1	PC	HTTP	インターネット	8001	80
192.168.0.2	IP端末1	PC	独自サービス	映像、音声	8002	6001
192.168.0.3	IP端末2	携帯端末	HTTP	インターネット	8003	80
192.168.0.3	IP端末2	携帯端末	RTSP	映像配信	8004	554

【図9】

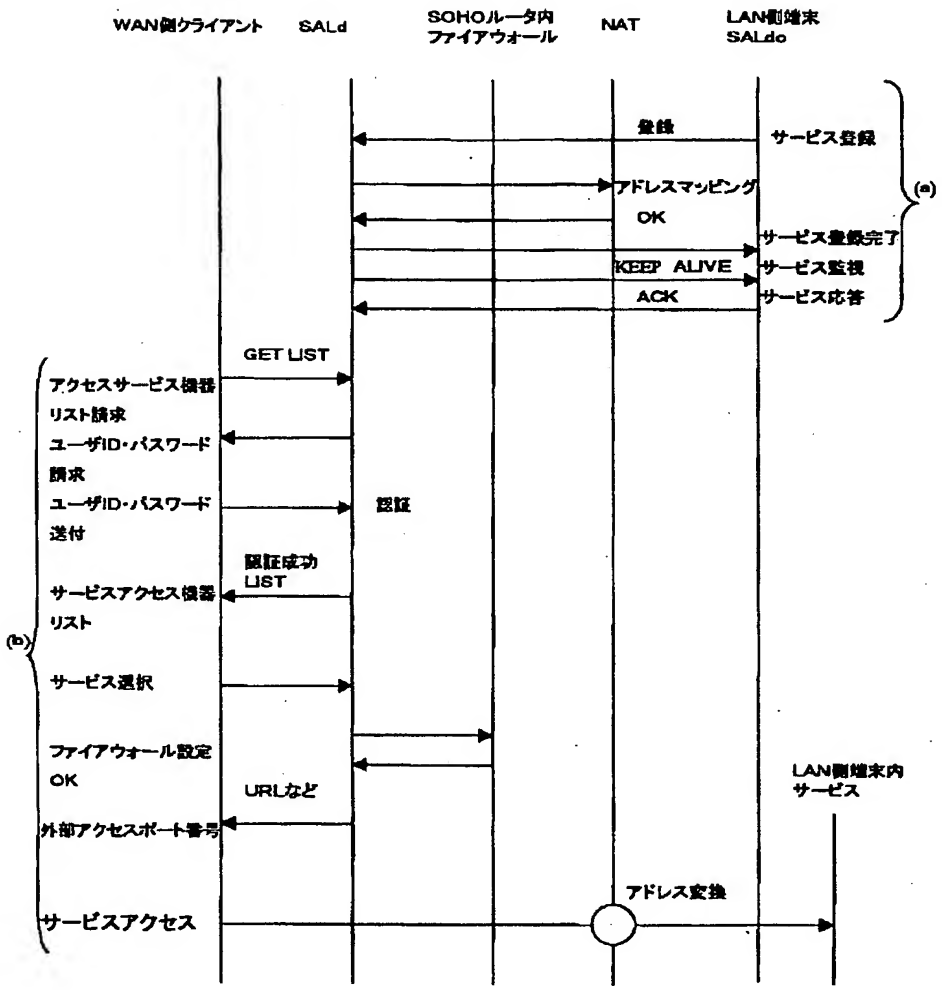
サービスアクセス権限リスト

端末名	端末属性	サービス名	サービス属性
IP端末1	PC	FTP	データ転送
IP端末1	PC	HTTP	インターネット
IP端末1	PC	独自サービス	映像、音楽
IP端末2	携帯端末	HTTP	インターネット
IP端末2	携帯端末	RTSP	映像配信

【図10】



【図13】



フロントページの続き

Fターム(参考) 5B089 GA04 GB02 HB02 KA13 KB06
KH03
5K030 GA11 HA08 HD03 HD07 HD09
JA11 JL07 JT03 KA01 KA02
KA13 KX30 MC09
5K034 AA17 BB06 DD03 FF11 HH01
HH02 HH65 JJ12 LL01 TT02